

ALGEBRA e LOGICA

(6 CFU)

prof. **Fabio Gavarini**

INSIEMI, CORRISPONDENZE, RELAZIONI, OPERAZIONI

Insiemi: Insiemi: definizione (naturale, o "ingenua"), descrizioni possibili; appartenenza e non appartenenza di elementi. Sottoinsiemi, sovrainsiemi. Inclusione tra insiemi; inclusione stretta. L'uguaglianza tra insiemi come doppia inclusione. L'insieme vuoto. L'insieme delle parti di un insieme. Famiglie: definizione, comparazione con gli insiemi. Partizioni di un insieme.

Operazioni tra insiemi: intersezione, unione, differenza, complementare, differenza simmetrica. Proprietà notevoli: (1) associatività e commutatività di intersezione, unione e differenza simmetrica; (2) leggi di De Morgan. Elementi speciali per le operazioni tra insiemi. Prodotto cartesiano tra insiemi.

Corrispondenze: Corrispondenze tra insiemi: definizione, esempi. Corrispondenza vuota, corrispondenza totale; corrispondenza identica. Immagine - tramite una corrispondenza data - di un sottoinsieme del dominio; controimmagine - tramite una corrispondenza data - di un sottoinsieme del codominio. Corrispondenza inversa; composizione - o prodotto (operatorio) - di due corrispondenze: definizione, esempi. Proprietà notevoli di inversione e composizione: associatività, esistenza di "elementi neutri", ecc.

Funzioni: Funzioni (o "applicazioni"): definizione, esempi, controesempi. Caratterizzazione delle famiglie come funzioni. Restrizione di una funzione ad un sottoinsieme del dominio. Funzioni iniettive; funzioni suriettive; funzioni biiettive. Caratterizzazione della biiettività di una funzione tramite la corrispondenza inversa (deve essere a sua volta una funzione). Esempi e controesempi. Composizione di funzioni: descrizione e proprietà (in generale). Funzioni invertibili: definizione; caratterizzazione in termini intrinseci (biiettività) e in termini della corrispondenza inversa (dev'essere a sua volta una funzione). Funzioni caratteristiche in un insieme. Biiezione naturale tra l'insieme delle parti di un insieme A e l'insieme delle funzioni caratteristiche in A .

Relazioni: Relazioni (binarie) in un insieme; operazioni insiemistiche tra relazioni; composizione, inversa, potenze di relazioni. Proprietà notevoli per una relazione: riflessiva, simmetrica, antisimmetrica, transitiva.

Relazioni di equivalenza: definizione, esempi. La congruenza modulo n tra numeri interi è una equivalenza. La relazione in X associata ad una funzione f da X a Y è una equivalenza. Generalizzazione: la relazione in X controimmagine, per una funzione f da X a Y , di una relazione in Y , è riflessiva, risp. simmetrica, risp. transitiva, se tale è la relazione iniziale in Y .

Classi di equivalenza; rappresentante di una classe di equivalenza; insieme quoziente, proiezione canonica. La biiezione naturale tra l'insieme delle equivalenze in X e l'insieme delle partizioni di X .

Insiemi con operazioni: Operazioni (binarie) in un insieme. Gruppoidi. Proprietà speciali di operazioni binarie. Unicità di elemento neutro (se esiste) e di elemento inverso (se esiste) di un elemento dato.

Semigrupperi, monoidi, gruppi. Il sottoinsieme degli elementi invertibili in un monoide è un gruppo (per la stessa operazione); esempi e controesempi; il monoide libero A^* (per la giustapposizione) su un insieme A (=linguaggio sull'alfabeto A); il gruppo delle permutazioni di un insieme (per la composizione).

Insiemi con due operazioni; casi speciali (semianelli, anelli, campi); esempi, controesempi. L'insieme delle parti di un insieme è anello commutativo unitario (non campo) per differenza simmetrica e intersezione.

Bibliografia: [Ca] [Capitolo I, paragrafi 1, 2, 3 e 4](#) - [G-P] files [Insiemi](#) , [Funzioni e cardinalità](#) , [Relazioni 1](#) , [Gruppi, anelli, campi](#) - [L-L] Chapters 1, 2 e 3; Appendix B - [PC] Capitolo 1, paragrafi 1, 2 e 3; Capitolo 4, paragrafo 1; Capitolo 5, paragrafi 1 e 2

Videolezioni: [Insiemi](#) , [Corrispondenze](#) , [Funzioni 1](#) , [Funzioni 2](#) , [Funzioni caratteristiche](#) , [Relazioni](#) , [Equivalenze 1](#) , [Equivalenze 2](#) , [Operazioni 1](#) , [Operazioni 2](#)

NUMERI NATURALI

Numeri naturali e Principio di Induzione: Il Sistema dei Numeri Naturali (=S.N.N.): definizione tramite assiomi di Peano. Il Principio di Induzione Debole (=Pr.I.D.). Il problema della esistenza e unicità di un S.N.N. (cenni). Relazione d'ordine (totale), somma e prodotto tra numeri naturali. L'insieme dei numeri naturali è un semianello (per somma e prodotto) in cui l'ordine è compatibile con le due operazioni.

Il Principio di Induzione Forte (=Pr.I.F.), il Principio del Minimo (=Pr.M.); l'equivalenza tra Pr.I.D., Pr.I.F. e Pr. M. (cenni). Dimostrazioni per induzione: idea, strategia operativa (base, passo induttivo).

Divisione euclidea e scrittura posizionale: Divisione con resto tra numeri naturali; dimostrazione per induzione in tre modi diversi: col Pr.I.D., col Pr.I.F. e col Pr.M.

Numerazione in base arbitraria: esistenza e unicità della scrittura posizionale (di un numero naturale) in base b (>1) arbitraria. Procedura operativa per il calcolo della scrittura posizionale.

Bibliografia: [AaVv] file [Numeri naturali \(D'Andrea\)](#) - [Ca] [Capitolo I, paragrafi 1 e 5](#) ; [Capitolo II, paragrafo 2](#) - [G-P] files [Induzione](#) , [Aritmetica sugli interi, etc. \(complementi\)](#), paragrafo 1 - [L-L] Chapter 1, section 8; Chapter 11, section 3 - [PC] Capitolo 1, paragrafo 4; Capitolo 2, paragrafo 10

Videolezioni: [Naturali](#) , [Induzione](#) , [Divisione](#) , [Numerazione](#)

CARDINALITÀ, NUMERI CARDINALI

Equipotenza tra insiemi; l'equipotenza è riflessiva, simmetrica, transitiva. Cardinalità di un insieme, numeri cardinali. Insiemi finiti, infiniti numerabili o infiniti non numerabili. Relazione d'ordine tra numeri cardinali; Teorema di Schroeder-Bernstein (*senza dimostrazione*).

Caratterizzazione degli insiemi infiniti: per un insieme X le seguenti proprietà sono equivalenti: (1) X è infinito, (2) esiste una funzione iniettiva dall'insieme dei numeri naturali ad X , (3) esiste un sottoinsieme proprio di X che è equipotente ad X stesso.

1° Teorema di Cantor: L'unione di una famiglia finita (non vuota) o numerabile di insiemi numerabili è numerabile - Applicazioni: \mathbf{Z} , \mathbf{Q} e $\mathbf{N} \times \mathbf{N}$ sono numerabili.

2° Teorema di Cantor: La cardinalità dell'insieme delle parti di un insieme è strettamente maggiore della cardinalità dell'insieme stesso.

I numeri cardinali infiniti superiori \aleph_n (per ogni n in \mathbf{N}). La cardinalità del continuo: $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})|$ (con cenni di dimostrazione). L'ipotesi del continuo generalizzata (cenni).

Bibliografia: [AaVv] file [Cardinalità \(D'Andrea\)](#) - [Ca] [Capitolo I, paragrafo 6](#) - [G-P] file [Funzioni e cardinalità](#), paragrafo 5 - [L-L] Chapter 3, section 7 - [PC] Capitolo 1, paragrafo 5

Videolezioni: [Cardinalità 1](#) , [Cardinalità 2](#)

NUMERI INTERI, CONGRUENZE, ARITMETICA MODULARE

Divisibilità e fattorizzazione tra interi: Richiami sui numeri interi, relazione coi naturali; operazioni, ordine, valore assoluto. Divisibilità, divisori, multipli; elementi invertibili, elementi associati. Elementi riducibili, elementi irriducibili. Il problema generale della fattorizzazione in un monoide: esempi di esistenza, controesempi all'unicità. Fattorizzazioni banali, fattorizzazioni equivalenti.

Teorema Fondamentale dell'Aritmetica: esistenza e unicità di una fattorizzazione in irriducibili per interi non nulli e non invertibili (*dimostrazione soltanto dell'esistenza*).

Teorema di Euclide: Esistono infiniti interi irriducibili a due a due non associati (*senza dimostrazione*).

Elementi primi; ogni primo è irriducibile. Massimo comun divisore (=MCD) e minimo comun multiplo (=mcm). Elementi coprimi (=primi tra loro).

Divisione euclidea tra interi (e conseguenze), equazioni diofantee: Divisione con resto tra numeri interi: esistenza e unicità di quoziente e resto (positivo). Esistenza del MCD in \mathbf{Z} , e identità di Bézout per esso: calcolo con l'algoritmo euclideo delle divisioni successive. Tra i numeri interi, ogni irriducibile è primo.

Teorema Fondamentale dell'Aritmetica: esistenza e unicità di una fattorizzazione in irriducibili per interi non nulli e non invertibili (*dimostrazione soltanto dell'unicità*).

Forma esplicita di $MCD(a,b)$ e di $mcm(a,b)$ in termini di fattorizzazioni di a e di b ; la relazione $MCD(a,b) mcm(a,b) = a b$; calcolo di $mcm(a,b)$ tramite il calcolo di $MCD(a,b)$.

Equazioni diofantee: definizione, criterio di esistenza di soluzioni, algoritmo per il calcolo di una soluzione.

Congruenze, aritmetica modulare: Congruenze in \mathbf{Z} (modulo n): ogni congruenza è una equivalenza. Descrizione delle classi di congruenza e dell'insieme quoziente \mathbf{Z}_n . Aritmetica modulare: compatibilità di somma e prodotto con ogni congruenza modulo n ; somma e prodotto in \mathbf{Z}_n .

Teorema: \mathbf{Z}_n è un anello commutativo unitario (*senza dimostrazione*).

Proposizione: \mathbf{Z}_n è un dominio $\Leftrightarrow n$ è irriducibile (=primo) $\Leftrightarrow \mathbf{Z}_n$ è un campo.

Criteri di divisibilità in \mathbf{Z} : strategia generale, esempi specifici.

Equazioni congruenziali e applicazioni: Equazioni congruenziali in \mathbf{Z} : definizione, connessione con equazioni in \mathbf{Z}_n , connessione con equazioni diofantee in \mathbf{Z} ; criterio di esistenza di soluzioni, algoritmo per il calcolo di una soluzione, insieme completo di soluzioni. Elementi invertibili in \mathbf{Z}_n ; criterio di invertibilità, calcolo dell'inverso tramite risoluzione di una equazione congruenziale. L'insieme $U(\mathbf{Z}_n)$ degli invertibili in \mathbf{Z}_n . Funzione di Eulero. Calcolo di potenze in \mathbf{Z}_n : generalità, il Teorema di Eulero (senza dimostrazione).

Sistemi di equazioni congruenziali: discussione, risoluzione - tramite il Teorema Cinese del Resto (senza dimostrazione) o tramite sostituzioni successive.

Bibliografia: [AaVv] files [Numeri interi \(D'Andrea\), paragrafo 4](#), [Congruenze, aritmetica modulare\(D'Andrea\), paragrafi 1 e 2](#) - [Ca] [Capitolo II, paragrafi da 1 a 6](#) - [G-P] files [Aritmetica sugli interi, congruenze, Teorema Cinese del Resto](#), [Aritmetica sugli interi, etc. \(complementi\)](#) - [L-L] Chapter 11, sections 1 to 9 - [PC] Capitolo 2, paragrafi da 1, 2, 3, 6, 7, 8 e 9

RETICOLI, ALGEBRE DI BOOLE, FUNZIONI BOOLEANE

Insiemi ordinati: Relazioni d'ordine: ordin(ament)i totali, ordin(ament)i buoni. Relazione di copertura e diagramma di Hasse. Sottoinsiemi ordinati, ordine prodotto. Principio di Dualità per insiemi ordinati.

Elementi minimali o massimali, minimo $\min(E')$ e massimo $\max(E')$ per un sottoinsieme E' in un insieme ordinato E . Minoranti, maggioranti, estremo inferiore $\inf(E')$ e estremo superiore $\sup(E')$ per un sottoinsieme E' in un insieme ordinato E . Unicità di $\min(E')$, di $\max(E')$, di $\inf(E')$ o di $\sup(E')$ - se esiste.

Reticoli: Reticoli: definizione come insiemi ordinati e definizione come insiemi con due operazioni binarie. Equivalenza delle due definizioni di reticolo (*idea della dimostrazione*). Esempi di reticoli.

Principio di Dualità per reticoli. Proposizione: Ogni reticolo finito è limitato. Complementi in un reticolo; reticoli complementati. Reticoli distributivi. Proposizione: In un reticolo distributivo, il complemento - se esiste - è unico, e valgono le Leggi di De Morgan per il complemento di $\inf(x,y)$ e di $\sup(x,y)$.

ν -Fattorizzazione in un reticolo; elementi ν -riducibili o ν -irriducibili; atomi. Proposizione: In un reticolo finito, ogni elemento ha una ν -fattorizzazione non ridondante in fattori ν -irriducibili.

Teorema di ν -Fattorizzazione Unica (in ν -irriducibili) per reticoli finiti distributivi.

Caratterizzazione degli elementi ν -irriducibili in un reticolo finito. Lemma: Ogni atomo è irriducibile.

Proposizione: In un reticolo finito unicamente complementato, ogni elemento ν -irriducibile è un atomo.

Teorema di ν -Fattorizzazione Unica (in atomi) per reticoli finiti distributivi complementati (=alg. di Boole).

Isomorfismi tra reticoli, reticoli isomorfi; proprietà degli isomorfismi. *Esempio:* \mathbf{D}_r è isomorfo a \mathbf{D}_s se e soltanto se r ed s hanno fattorizzazioni in primi distinti che coinvolgono gli stessi esponenti.

Sottoreticoli di un reticolo. Teorema: Un reticolo è distributivo se e soltanto se non ha sottoreticoli isomorfi a \mathbf{N}_5 o a \mathbf{M}_5 (*senza dimostrazione*).

Algebre di Boole: Algebre di Boole: definizione come reticoli distributivi (limitati) complementati, definizione come insiemi con due operazioni particolari. Equivalenza delle due definizioni (*senza dimostrazione*). Il *Principio di Dualità* per algebre di Boole. *Controesempi:* gli insiemi totalmente ordinati con più di due elementi non sono algebre di Boole. *Esempi di algebre di Boole:* l'insieme delle parti $P(X)$; le funzioni a valori in un'algebra di Boole; prodotti di algebre di Boole; i prodotti $\{0,1\}^n$.

Isomorfismi tra algebre di Boole, algebre di Boole isomorfe; proprietà degli isomorfismi. *Esempio:* la biiezione canonica da $P(X)$ a $\{0,1\}^X$ - per ogni insieme X - è un isomorfismo di algebre di Boole.

Teorema (Stone - caso finito): Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi. *Corollario:* Ogni algebra di Boole finita è isomorfa all'insieme delle funzioni caratteristiche dell'insieme dei suoi atomi. In particolare, la cardinalità di un'algebra di Boole è sempre una potenza di 2.

Funzioni booleane, polinomi booleani: L'insieme $F_n(B)$ delle funzioni booleane in n variabili su un'algebra di Boole B ; struttura di algebra di Boole. L'insieme P_n dei polinomi booleani in n variabili; funzioni booleane indotte da un polinomio booleano. L'insieme $P_n(B)$ delle funzioni polinomiali su B indotte da un polinomio booleano; $P_n(B)$ è sottoalgebra di Boole di $F_n(B)$.

Equivalenza tra polinomi (quando inducono la stessa funzione su $\underline{2}:=\{0,1\}$). *Teorema:* Due polinomi booleani inducono la stessa funzione booleana su qualsiasi algebra di Boole se e soltanto se sono equivalenti.

Prodotti, prodotti fondamentali (in P_n); somme di prodotti (ridondanti, non ridondanti, complete); passaggio da un oggetto (prodotto o somma) non "buono" (fondamentale, o irridondante, o completo) ad uno "buono" equivalente. Forma normale disgiuntiva di un polinomio booleano: esistenza e unicità. Dualizzazione: la forma normale congiuntiva di un polinomio booleano. Metodi operativi per il calcolo della F.N.D. di un polinomio booleano: (1) tramite "tavole di verità", (2) tramite manipolazioni successive.

Relazione di "maggior semplicità" tra polinomi booleani equivalenti che siano somme di prodotti. Definizione di *forma minimale* di un polinomio booleano; esistenza (e non unicità) di forme minimali. La relazione di "implicazione" tra polinomi booleani. Il legame tra la relazione di *implicazione* e quella di *equivalenza*. Gli implicanti primi di un polinomio booleano.

Proposizione: Ogni somma di prodotti è equivalente alla somma di tutti i suoi implicanti primi.

Somme di prodotti irridondanti. *Proposizione:* Ogni forma minimale di un polinomio booleano f è somma irridondante di implicanti primi di f . Il *consenso* di due prodotti in P_n . Il *Metodo del Consenso:* algoritmo di calcolo della somma di tutti gli implicanti primi di un polinomio booleano in n variabili (*senza dimostrazione*). Calcolo di una forma minimale tramite il *Metodo del Consenso*.

Bibliografia: [Ca] [Capitolo I, paragrafo 3\(B\)](#) - [G-P] files [Relazioni - 2](#) , [Reticoli](#) , [Algebre di Boole](#) , [Funzioni booleane](#) , [Forme minimali di una funzione polinomiale](#) - [L-L] Chapter 14, sections 1 to 5 and 7 to 11; Chapter 15, sections 1 to 9

Videolezioni: [Insiemi ordinati](#) , [Reticoli 1](#) , [Reticoli 2](#) , [Reticoli 3](#) , [Algebre di Boole 1](#) , [Algebre di Boole 2](#)

FUNZIONI RICORSIVE, EQUAZIONI ALLE DIFFERENZE

Funzioni ricorsive: Funzioni (o "successioni") ricorsive; dati iniziali, equazione ricorsiva e grado associati. *Teorema di Ricorsione:* Esiste un'unica funzione che soddisfi una data equazione ricorsiva e abbia dati iniziali assegnati. Casi speciali: funzioni ricorsive lineari, lineari omogenee, lineari a coefficienti costanti.

Proposizione: L'insieme S delle successioni che sono soluzioni di un'equazione ricorsiva lineare omogenea di grado k è sottospazio vettoriale dello spazio di tutte le successioni, e ha dimensione k (*cenni di dimostrazione*).

Strategia di calcolo di una funzione ricorsiva lineare omogenea: ricerca di una base dello spazio delle soluzioni dell'equazione ricorsiva associata, e successiva imposizione delle condizioni iniziali.

Equazioni ricorsive lineari omogenee a coefficienti costanti: Calcolo esplicito di funzioni (reali o complesse) ricorsive lineari omogenee a coefficienti costanti omogenee nei casi di grado 1 e di grado 2.

Bibliografia: [G-P] file [Equazioni alle differenze finite \(cenni\)](#) - [L-L] Chapter 3, section 6; Chapter 6, sections 6, 7 and 8

Videolezioni: [Funzioni ricorsive 1](#) , [Funzioni ricorsive 2](#) , [Funzioni ricorsive 3.1](#) , [Funzioni ricorsive 3.2](#)

TESTI (libri, dispense, videolezioni, ecc.) consigliati:

- [AaVv] - Autori Vari, [Materiale vario disponibile in rete](#) (per gentile concessione degli autori) -
- alla pagina http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat.html#Mat-Dis_altro-mat
- [Ca] - G. Campanella, [Appunti di Algebra 1](#) (per gentile concessione dell'autore) -
- alla pagina http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/dispense-ecc/Algebra_1_-_dispense_di_Campanella.rar
- [Ga] - F. Gavarini, [Videolezioni varie](#) -
- alla pagina <http://didattica.uniroma2.it/files/index/insegnamento/144372>
- [G-P] - L. Geatti, G. Pareschi, [Appunti vari](#) (per gentile concessione degli autori) -
- alla pagina [http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/Algebra-Logica_\(ING-INF\)/Pagina_Web_Algebra-Logica_2012-13/AL_2012-13.html#app_alg-log](http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/Algebra-Logica_(ING-INF)/Pagina_Web_Algebra-Logica_2012-13/AL_2012-13.html#app_alg-log)
- [L-L] - S. Lipschutz, M. Lipson, *Discrete Mathematics*, 3rd Edition, Schaum's Outlines, McGraw-Hill, 2007
- [PC] - G. M. Piacentini Cattaneo, *Algebra - un approccio algoritmico*, ed. Decibel/Zanichelli, Padova, 1996
-